Примена машинског учења у статичкој верификацији софтвера

Семинарски рад у оквиру курса
Методологија стручног и научног рада
Математички факултет

Лазар Ранковић, Немања Мићовић, Урош Стегић
lazar.rankovic@outlook.com, nmicovic@outlook.com, mi10287@alas.matf.bg.ac.rs

Абстракт

Испитивање исправности програма представља значајну област рачунарства. Експанзија научних као и софтверских решења може имати како позитнивних тако и негативних последица. С тога је потребно поседовати механизам којим се може испитати исправност програмског кода. Међутим, због неодлучивости Халтинг проблема и других ограничења, јављају се различити проблеми приликом испитивања исправности софтвера. Технике машинског учења проналазе све већу примену у различитим областима рачунарства, и примећено је да се неки од проблема статичке верификације могу ефикасно решити применом ових техника. Овај рад ће дати преглед одређених проблема статичке верификације, као и механизме машинског учења који су постигли значајна побољшања.

Садржај

1 Uvod

Рачунарски системи имају све значајнију примену у нуклеар. Софтвер који контролише то мора да буде исправан јер мале грешке у софтверу могу бити скупе или опасне по живот. Из овог разлога је област верификације софтвера верома значаја. Последњих година су достигнути велики напреци у развоју алата за верификацију, али као и свугде, постоје проблеми који се тешко решавају. Анализа програмског кода се заснива на математичким моделима. У неким ситуацијама је коришћење стриктних математичких механизама тешко или чак немогуће за аутоматизацију. Са друге стране област машинског учења постиже високе резултате на пољу ???. Учење на основу искуства је кул. Технике машинског учења данас имају широку примену, а неке од њих су у оквиру статичке верификације софтвера. У раду ће бити дат преглед примена неких техника машинског учења у решавању одређених проблема верификације.

2 Верификација софтвера

Верификација софтвера је дисциплина развоја софтвера која за циљ има провераву да ли програм задовољава све унапред задате захтеве. Ти захтеви су представљени спецификацијом свих жељених особина програма и дефинишу се пре процеса верификације. Највећа примена верификације софтвера је у оптимизацији кода и провери исправности.

Потребно је направити разлику између тоталне и делимичне исправности. Испитивање тоталне исправности захтева да се за све могуће улазе покаже заустављање програма. Доказ заустављања у општем случају није могуће извести [13]. Такође, испитивање нетривијалних семантичких својстава је неодлучив проблем [1]. Према томе, у рачунарству је довољно испитати делимичну исправност софтвера, тј. довољно је показати да ће резултат извршавања програма бити валидна вредност.

Два приступа при верификацији софтвера су *динамичка верификација* и *статичка верификација* [6]

- **Динамичка верификација**
  Овај вид верификације се врши у току извршавања програма и то најчешће скупом унапред припремљених тестова који морају бити испуњени. Очигледно је да због неисцрпне варијације могућих улаза, овај вид тестирања нема за циљ валидацију програма, већ је циљ динамичке верификације проналажење грешка на неком не тривијалном скупу тестова.
- **Статичка верификација**
  Статичка верификација софтвера подразумева анализу софтвера без његовог извршавања, тачније анализу кода применом неке од техника које ће бити описане у наставку. Анализу кода може обављати човек, а може се и аутоматизовати. Аутоматизација подразумева описивање (па чак и превођење) кода језиком изабране математичке теорије.

У наставку ће бити више речи о статичкој верификацији. Биће описани механизми анализе кода, технике верификације и чести проблеми овог типа верификације.

3 Технике статичке верификације

Претходним поглављем су дефинисани основни појмови верификације софтвера. Предочено је да је немогуће у општем случају испитати заустављање програма и анализирати нетривијална семантичка својства. Ово поглавље ће дати увид у аутоматизоване технике статичке анализе.

3.1 Апстрактна интерпретација

Апстрактна интерпретација је теорија семантичке апроксимације чија је идеја да изгради нову семантику над програмским језиком тако да се конкретан програм увек завршава. Тако се анализа програма врши над апстрактном семантиком да би се добила апроксимација над целом семантиком. Коришћење апстрактне интерпретације се омогућава помоћу две функције: функције која пресликава конкретне вредности у апстрактне вредности и функције која слика апстрактне вредности у конкретне вредности. Неизбежно је заобићи губљење података при пресликавању из конкретних вредности у апстрактне вредности јер је циљ показати да се над апострактном семантиком програм завршава. Користећи овај математички оквир је релативно лако показати да ако се програм завршава у новој семантици програм ће бити коректан и у стварној семантици.

3.2 Симболичка анализа

Симболичка анализа је метод статичке анализе који анализира програмске вредности који могу да се мењају. Овај метод има за циљ да изведе математички модел који прецизно описује израчунавање, заправо може се посматрати као нека врста компајлера који преводи програм у симболичке изразе. Квалитет алгебарских система као што су (Axiom, Derive, Macsyma, Maple, Mathematica, MuPAD, and Reduce) је веома битан јер квалитет овог начина анализе у великој мерим зависи од паметних алгебарских упрошћавања.

3.3 Проверавање ограничених модела

Проверавање ограничених модела (енг. Bounded model checking) је техника верификације која се највише користи у индустрији полупроводника, тачније верификација логичкх кола. Укратко речено смисао је да се логичка кола опишу исказном логиком. Следећи корак је провера задовољивости добијене исказне формуле. Испитивање задовољивости формула је НМ-тежак проблем, и за решавање овог питања користе се сат решавачи. Ефикасност сат решавача је од кључног значаја за ову технику. Ова техника је такође примењљива и за анализу софтвера, један од начина примене је посматрање извршавања целокупног програма као скупа стања, односно као један коначни аутомат у ком се прелази из стања у стање. Ако се тако посматра програм могуће је описати сва стања искасном логиком затим повезати сва стања и тако добијену формулу пустити у сат решавач. Резултат сат решавача је може бити формула је задовољива сто би значило да је програм коректан или ако је формула незадовољива резултат ће бити контрапример којим се показује да програм није коректан и може представљати основу за дебаговање.[14][5].

НЕКИ ЗАКЉУЧАК ОВДЕ

4 Машинско учење

У претходним поглављима је описана статичка верификацију софтвера. Показана је важност те области и изложене су технике верификације. Ово поглавље ће приближити област машинског учења и описаће главне аспекте ове дисциплине,

4.1 Основе машинског учења

Дефиниција 1. *"За програм кажемо да учи из искуства E кроз обављање задатка T са мером квалитета P, ако повећањем искуства E расте мера P за обављен задатак T."*

— Tom M. Mitchell *[9]*

Машинско учење се може посматрати као област рачунарства која се бави анализом алгоритама који генерализују. Са практичног аспекта, генерализација може значити уопштавање закона над датим подацима.

Три најзначајније подобласти машинског учења су: *надгледано учење*, *ненадгледано учење* и *учење условљавањем*. Подаци из којих алгоритми машинског учења уче, могу бити обележени, необележени и могу се генерисати у фази учења. Оваква природа података је основ за разликовање три наведене подобласти.[9].

Међу многим проблемима над којима су често примењивани алгоритми машинског учења, истактнути су проблем регресије и проблем класификације. Под проблемом класификације се подразумева испитивање датог објекта и одређивање класе којој он припада на основу његових својстава (атрибута). Типичан пример класификације је одређивање порекла тумора на основу његове величине. Проблем регресије представља предвиђање понашања непрекидне променљиве. Пример регресије је предикцију цене стамбеног објекта на основу његове величине, броја соба и разних других релевантних карактеристика.

Пре примене машинског учења потребно је проучити проблем који се решава, уочити његове специфичности и припремити и анализирати податке из којих ће алгоритми учити. Након детаљне анализе, врши се одабир одговарајућег математичког модела. Изабрали модел се даље тренира над подацима. Тренинг се понавља довољан број пута при чему у свакој итерацији модел евалуира тј. мери се грешка коју тај модел прави. Након сваког мерења, у зависности од алгоритма, врши се корекција модела у циљу минимизације грешке.

У даљем тексту ће бити приказани конкретни алгоритми који су релевантни за процес верификације и дискутоваће се о њиховим својствима.

4.2 Значајност машинског учења

Конвенционалан начин решавања проблема у рачунарству се своди на формално дефинисање низа корака који улазне параметре трансформишу не би ли дошли до резултата. Овакав приступ је користан у ситуацијама када је потребно решити проблеме који су човеку изазовни, као што су компликоване рачунске операције, сортирање великих низова и томе слично. Поставља се питање: како написати

програм који би обављао задатке које човек свакодневно лако обавља? На пример, да ли је могуће написати програм који би био у стању да препознаје објекте са фотографија?

Рачунарски вид (енг. computer vision) је дисциплина која се бави овим проблемом.[4]. Алгоритми који су примењивани пре раста популарности машинског учења нису показали значајне резултате. Могли су да генеришу једноставне геометријске моделе који нису давали задовољавајуће резултате. Дубоке неуронске мреже су алгоритами машинског учења који су показали значајне напретке у овој области [2].

Класификација дела програма на валидна стања и она која могу резултовати грешком је од кључног значаја за ефикасност алата за верификацију [3] [7]. Конкретним проблемима и њиховим решењима ћемо се бавити у наредним поглављима.

4.3 Технике машинског учења

О општој слици примене алгоритама машинског учења је било више речи у уводном делу овог поглавља. Како је проблем класификације централни проблем над којиме се примењује машинско учење у статичкој верификацији, биће представљена два алгоритма која решавају тај проблем. Зарад потпуности, биће описан и један алгоритам решавања регресионих проблема.

Линеарна регресија

Као што је речено у уводном делу, регресиони проблем представља предвиђање циљне променљиве непознате инстанце на основу осталих њених атрибута. Нека је y_i циљна променљива, а $\vec{x} = (x_1, x_2, ..., x_n)$ вектор атрибута. У примеру предикције вредности куће то могу бити број соба, квадратура куће итд. Инстанца из скупа података ће онда бити $(\vec{x}_i, y_i)$. Модел линеарне регресије, параметризован вектором w, који описује законитост је следећи:

$$h(\vec{x}_i) = w^T \cdot \vec{x}_i \tag{1}$$

Грешка коју модел прави је потребно представити погодним избором функције грешке $L(w)$. Чест избор ове функције је средњеквадратна грешка коју модел прави над свим инстанцама из тренинг скупа.

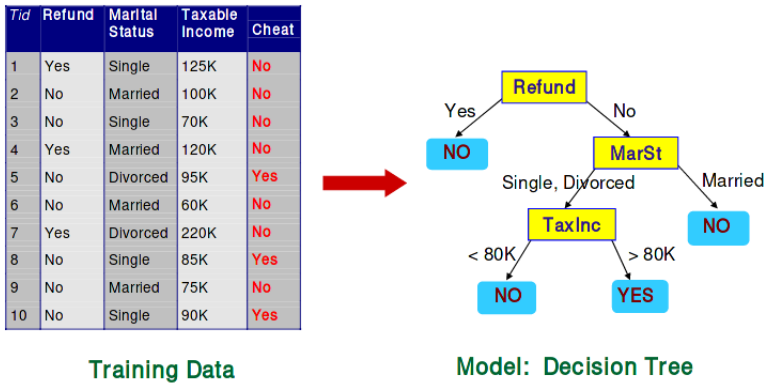
$$L(w) = \frac{1}{N} \sum_{i=1}^{N} (h(\vec{x}_i) - y_i)^2 \tag{2}$$

Тренинг се врши тако што се одређеном оптимизационом техником минимизује функција грешке по параметрима w.

Стабла одлучивања

Стабла одлучивања представљају један од основних метода класификације. Употребу стабала одлучивања оправдава њихова висока интерпретабилност [11]. У листовима стабла одлучивања се налазе вредности циљне променљиве, односно у случају класификације, класе којима инстанца може припасти. Унутрашњи чворови стабла представљају атрибуте по којима се врши подела. Када су ти атрибути категоричког типа, потомци датог чвора су добијени из свих могућих вредности које тај категорички атрибут може имати. У случају

да је атрибут некатегоричког типа, најчешће се врши подела могућих вредности на дисјунктне интервале тако да свако дете тог чвора одговара једном од интервала. Слика 1 приказује једно могуће стабло одлучивања добијено на основу података.



Слика 1: Стабло одлучивања

Метода потпорних вектора

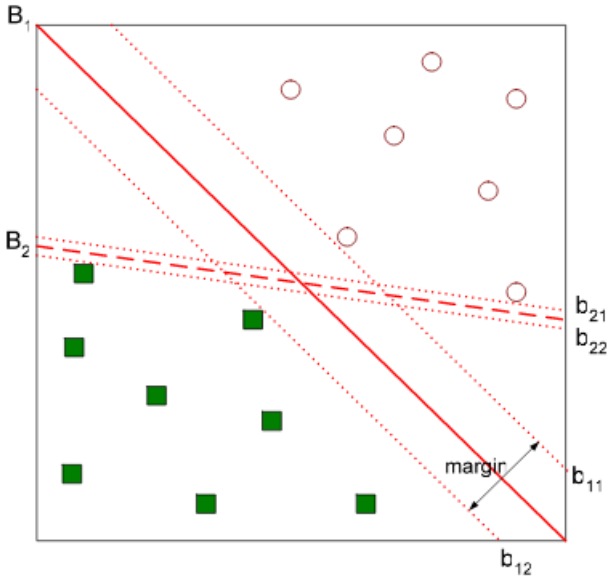
Проблем класификације се може разматрати у следећем контексту. Инстанце које се класификују су представљене тачкама у неком високодимензионалном простору. Бинарни класификатор је хиперраван која дели простор на два дела, тако да се у једном делу простора нађу све инстанце које припадају једној класи, а у другом делу ће се наћи оне које припадају другој класи. Раздвајајућих хиперравни може бити више, па је зато потребно одабрати хиперраван која боље описује поделу међу подацима [10].

Маргина класификације је најмање растојање између тачака које се налазе у различитим потпросторима и бинарног класификатора. Слика 2 приказује хиперравни B_1 и B_2. Прва хиперраван боље раздваја податке. Маргина $(b_1 1, b_1 2)$ је значајно већа од маргине (b_{21}, b_{22}) и то је оно што први класификатор чини знатно бољим.

Максимизацијом маргине се добија класификатор који боље описује поделу. Зарад конвенције, проблем максимизације се своди на проблем минимизације, те се добија следећи оптимизациони проблем:

$$\min_{w,w_0} \frac{\|w\|^2}{2} \tag{3}$$

Линеарна регресија, стабла одлучивања и метод потпорних верктора су приказани у овом поглављу због својих примена у проблемима статичке верификације. Поглавље шест се бави овим применама. Следеће поглавље ће представити релевантне проблеме верификације и даће основ за примену ових метода.



Слика 2: Приказ различитих хиперравни

5 Одабрани проблеми статичке верификације

До сада смо видели стандардне проблеме и технике статичке верификације и машинског учења. У овом поглављу ћемо издвојити значајне проблеме верификације на које су, применама алгоритама машинског учења постигнути значајнији резултати.

Статичка верификација мора бити у стању да разликује позитивна стања програма од негативних. Негативна су она која доводе програм до грешке. *Интерполантама* (енг. interpolants) називамо предикате који раздвајају позитивна од негативних стања. У статичкој верификацији се коришћењем оваквих интерполанти гради даљи доказ. Показано је да се ове интерполанте могу интерпретирати као бинарни класификатори. Проблем који се овде јавља је генерисање интерполанти, тј проналажење одговарајућег класификатора [12]. У делу 6.1 детаљније је описан приступ коришћен у [12].

Поред итерполанти, могуће је препознати нетривијална својства програма која даље резултују грешком. Грађењем *класификатора нетачне инваријанте* (енг. False Invariant Classifier) је могуће рангирати својства програма по томе колику вероватноћу за грешком та својства проузрокују. Одређивање нетривијалног својства датог програма је у општем случају неодлучив проблем [13, 3].

Код апстрактне интерпретације је остварив баланс између прецизности изгенерисане инваријанте и скалабилности система за верификацију. Овај баланс је последица детаљне анализе апстрактног синтаксног стабла. Одабир инваријанте је тежак проблем и показано је да се може утврдити тестирањем [12, 7].

Проблеми које смо представили овим поглављем су решена користећи одговарајуће технике машинског учења. У наредом поглављу

ћемо се бавити тим решењима, даћемо увид у начине на који су та решења примењена и покушати да одговоримо на питање како наставити усавршавање тих техника.

6 Неке примене техника машинског учења у статичкој верификацији

Ово је есенција. Одабирају се проблеми из претходног поглавља и показује се како се решава. Прво иде неки уводни део, онда из литературе се покупе те технике и таксативно се наводе (принцип проблем-решење).

6.1 Проналажење интерполанти

Неформално говорећи, интерполанта представља предикат који раздваја позитивна стања програма од негативних. Примена машинског учења у проналажењу интерполанти огледа се у добијању модела који представља саму интерполанту. У делу 6.1.1 изложене су основе из [12] базиране на методу потпорних вектора, док је у делу 6.1.2 изложен приступ из рада [7] базиран на стаблима одлучивања. Експериментални резултати показали су да приступи базирани на машинском учењу јесу упоредиви са традиционалним техникама.

6.1.1 Проналажење интерполанти користећи метод потпорних вектора

Нека су A и B формуле у теорији линеарне аритметике [8].

$$\phi ::= w^T x + d \geq 0 \mid true \mid false \mid \phi \wedge \phi \mid \phi \vee \phi \mid \neg\phi \tag{4}$$

При чему је $\vec{w} = (w_1, ..., w_n)^T \in R^n$ вектор константи у простору R^n; $\vec{x} = (x_1, ..., x_n)^T$ вектор променљивих из простора R^n.

Дефиниција 2. *Интерполанта за пар формула (A, B) тако да* $A \wedge B \equiv \bot$ *је формула* I *која задовољава* $A \Rightarrow I, I \wedge B \equiv \bot$ *при чему формула* I *садржи само променљиве које се јављају у формулама* A *и* B.

На слици 3 приказан је програмски код који ће бити коришћен као илустрација. Функција непознат број пута инкрементира променљиве x и y, потом их декрементира све док променљива x не постане 0. Коначно, уколико је $y \neq 0$ онда програм одлази у стање грешке. Приметимо да је инваријанта $x = y$ довољна да се докаже да програм никад неће доћи у стање грешке.

Претпоставимо да је функција `foo()` извршила на следећи начин (у заградама су хронолошки наведени линије инструкција): $(1, 2, 3, 2, 4, 5, 4, 6, 7)$ који води у стање грешке. Поделимо ток на два скупа, A и B и пронађимо интерполанте за наведени ток.

Скуп A садржи вредности x и y које се добијају након извршавања линија 1, 2 и 3. У скупу B се налазе оне вредности x и y које би се добиле уколико би програм извршио линије 4, 5, 6 и 7 чиме би програм дошао у завршно стање.

Имамо да $A \wedge B \equiv \bot$ при чему важи:

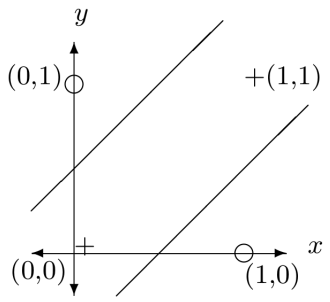
```
foo( )
{
1:  x = y = 0;
2:  while (*)
3:   { x++; y++; }
4:  while ( x != 0 )
5:   { x--; y--; }
6:  if ( y != 0 )
7:    error() ;
}
```

Слика 3: Пример кода

$$A \equiv x_1 = 0 \wedge y_1 = 0 \wedge if\_then\_else(b,\ x = x_1 \wedge y = y_1,\ x = x_1 + 1 \wedge y = y_1 + 1)$$
$$B \equiv if\_then\_else(x = 0,\ x_2 = x \wedge y_2 = y,\ x_2 = x - 1 \wedge y_2 = y - 1) \wedge x_2 = 0 \wedge \neg(y_2 = 0)$$

A представља скуп достижних стања док B представља скуп стања која воде у стање грешке. Интерполанта је доказ да су скупови A и B дисјунктни и изражава се користећи заједничке промењиве из скупова A и B. Затим, помоћу доказивача теорема се рачунају вредности за (x, y) које задовољавају формуле A и B [12].

Добијене вредности представљају скуп инстанци над којим се може тренирати класификациони модел (попут логистичке регресије или потпорних вектора). Позитивне инстанце представљају вредности промењивих које задовољавају формулу A и аналогно, негативне инстанце представљају вредности промењивих које задовољавају формулу B.



Слика 4: Класификација у тражењу интерполанти

Слика 4 приказује вредности промењивих (x, y) за A као плусеве (тачке $(0, 0)$ и $(1, 1)$) и B као кружиће (тачке $(1, 0)$ и $(0, 1)$). Приказани модел је добијен коришћењем метода потпорних вектора. Резултујуће праве одговарају једначинама:

$$e_1 : 2y = 2x + 1$$
$$e_2 : 2y = 2x - 1$$

Интерполанта која се одавде може извести је

$$2y \leq 2x + 1 \wedge 2y \geq 2x - 1$$

Табела 1: Добијене интерполанте на неким од познатијих тест примера у области.

Датотека	Време (с)	Интерполанта
f1a	0.022	((y = 1 | x <= 0) & x = 1) | (y = 0 & (y = 1 | x <= 0))
ex1	0.021	xa + 2*ya >= 0 | xa + 2*ya >= 5 | xa + 2*ya >= 5
f2	0.20	y <= 3*x | y <= 3*x + 1 | y <= 3*x + 1
nec1	није доступно	Није пронађена
nec2	0.018	x < y (исто)
nec3	0.016	y <= 9 (исто)
nec4	0.021	(x = y | y = 0) | (y = x) | (y = x)
nec5	0.018	s >= 0 (исто)
pldi08	0.017	y > x
fse06	0.017	y + x >= 0 & y >= 0 & y >= 0 & y >= 0

Овај предикат представља инваријанту чијим доказивањем се показује да програм не може доћи у стање грешке. Једноставнија интерполанта $x = y$ се може добити транслирањем добијених правих што ближе позитивним истанцама, докле год се одржава сепарабилност позитивних и негативних инстанци.

Табела 1 приказује резултате из [12] на неким од познатих примера. Интерполанте које су означене са *исто* су интерполанте које су добијене користећи решавач OpenSMT.

6.1.2 Проналажење интерполанти користећи стабла одлучивања

Интерполанте се могу извести и другим методима машинског учења. Рад [7] илуструје приступ који користи стабла одлучивања. За програмски код се генеришу позитивне и негативне инстанце над којима се гради стабло одлучивања користећи похлепни алгоритам. Правила добијена у стаблу се трансформишу у формулу која се потом проверава да ли је инваријанта користећи SMT решавач.

Резултати су показали да једноставни похлепни алгоритам који гради стабло даје и једноставне формуле за интерполанте. Стабло је лако научило комплексне бинарне инваријанте као једноставне конјункције.

Слика 5 приказује пример програма и његова стања која се могу добити на основу покретања самог програма. Добра стања можемо добити пратећи претпоставке (линија 2), бележећи ток променљивих и провером да ли је испуњен услов $x \neq 0$ са линије 12. Лоша стања можемо добити игноришући услов са линије 2. На пример, тачка $(-2, -2)$ тачка $(-4, -4)$ представљају лоша стања.

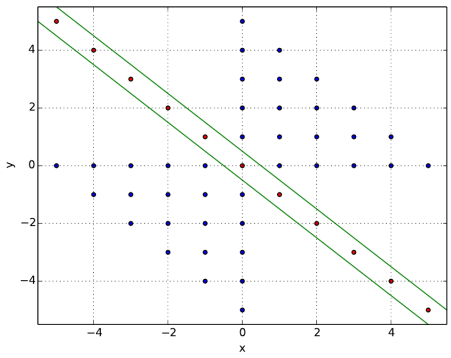
Слика 6 приказује стабло добијено применом алгоритма описаног у [7]. Добијени алгоритам је сложености $O(mn \log(n))$, где је m број атрибута а n број инстанци.

6.2 Грађење класификатора нетачне инваријанте

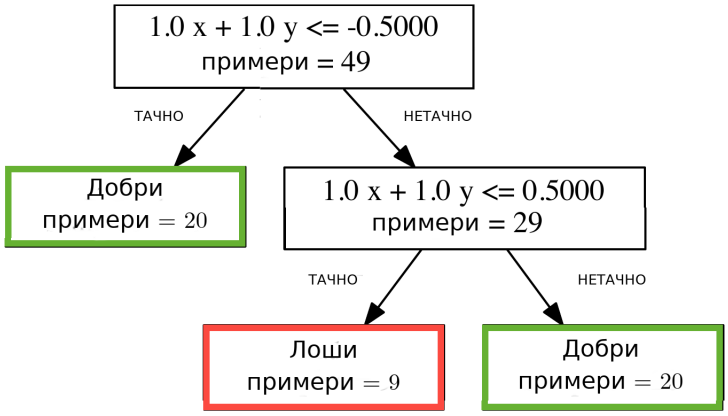
7 Закључак

Овде машти на вољу.. :)

```
1  var x, y: Int;
2  assume x = 0 ∧ y ≠ 0;
3
4  while (y ≠ 0) {
5    if (y < 0) {
6      x := x − 1; y := y + 1;
7    } else {
8      x := x + 1; y := y − 1;
9    }
10 }
11
12 assert x ≠ 0;
```



Слика 5: Пример програма. Лева страна приказује код, десна страна садржи добра стања (плаве тачке) и лоша стања (црвене тачке).



Слика 6: Стабло одлучивања добијено за пример са слике 5.

Литература

[1]

[2] Deep image: Scaling up image recognition. *CoRR*, abs/1501.02876, 2015. Withdrawn.

[3] Yuriy Brun. Finding latent code errors via machine learning over program executions, 2004.

[4] Christopher M. Brown Dana H. Ballard. *Computer vision*. Prenice-Hall, Inc., 1982.

[5] Vijay D'Silva, Daniel Kroening, and Georg Weissenbacher. A survey of automated techniques for formal software verification. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 27(7):1165–1178, July 2008.

[6] Milena Vujosevic Janicic. Regresiona verifikacija softvera korišćenjem sistema lav.

[7] Siddharth Krishna, Christian Puhrsch, and Thomas Wies. Learning invariants using decision trees. *CoRR*, abs/1501.04725, 2015.

[8] Daniel Kroening and Ofer Strichman. *Linear Arithmetic*, pages 111–147. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[9] Tom M. Mitchell. *Machine Learning*, volume 1. McGraw Hill, 1997.

[10] John Shawe-Taylor Nello Christianini. *An introduction to support vector machines*, volume 1. Cambridge university press, 2000.

[11] David Landgrebe S. Rasoul Safavian. A survey of decision tree classifier methodology, 1991.

[12] Rahul Sharma, Aditya V. Nori, and Alex Aiken. Interpolants as classifiers.

[13] Alan M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 2(42):230–265, 1936.

[14] Wolfgang Wögerer and Technische Universität Wien. A survey of static program analysis techniques, 2005.